

DOCKET FILE COPY ORIGINAL

Before the
Federal Communications Commission
Washington, D.C.

RECEIVED

DEC 12 1997

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of

Communications Assistance
for Law Enforcement Act

)
)
)
)
)

CC Docket No. 97-213

COMMENTS OF OMNIPOINT COMMUNICATIONS, INC.

Omnipoint Communications, Inc. ("Omnipoint"), by its attorneys, file these comments in response to the Commission's October 19, 1997 Notice of Proposed Rulemaking ("NPRM") in the above-captioned proceeding. Omnipoint and its affiliates are small business licensees operating broadband Personal Communications Services ("PCS") systems in the New York Major Trading Area and several other Basic Trading Areas, and hold PCS licenses to serve over 96.5 million people in the United States. According to U.S. Department of Justice statistics, Omnipoint's service areas include jurisdictions where very high volumes of wiretaps and other forms of electronic surveillance are conducted annually. Indeed, Omnipoint already has assisted law enforcement officials to conduct lawful electronic surveillance in numerous situations.

Although Omnipoint is a relatively new telecommunications carrier, it has gained substantial experience in the area of working cooperatively with law enforcement authorities. As a relatively new entrant, it has approached its responsibilities from a fresh perspective. Omnipoint protects its subscribers' constitutionally protected privacy by examining closely its statutory obligations, unimpeded by traditional views of how carriers *should* behave.

With this background, Omnipoint believes that in prescribing rules to implement the Communications Assistance for Law Enforcement Act ("CALEA")—particularly those governing the internal policies of carriers—the Commission needs to strike a balance that promotes a certain degree of responsible uniformity among carriers without imposing undue

No. of Copies rec'd
List ABCDE

06

burdens and impractical procedures. Omnipoint's comments elaborate on how the Commission can achieve CALEA's objectives without micromanaging carrier operations. Its comments also address CALEA's definition of "telecommunications carrier" and criteria for Commission grants of extensions of compliance dates.

I. Carrier Security Policies and Procedures

A. Preliminary Observation

The NPRM repeatedly refers to "interceptions" and "interception activities." It is important to note that the term "interception" refers to only one means of electronic surveillance. It refers to certain "real time" acquisitions of the content of voice or data communications transmitted over telecommunications facilities. *See* 18 U.S.C. § 2510(4). *See also* Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994).

CALEA and state and federal wiretap laws cover a wider range of electronic surveillance than only "interceptions." For example, important aspects of CALEA refer to the capture of dialing information and other "call-identifying information." *See, e.g.*, 47 U.S.C. § 1001(2). In addition, the Electronic Communications Privacy Act of 1986 added provisions addressing the accessing of "electronic communications in electronic storage," such as electronic mail or voice mail messages. *See, e.g.*, 18 U.S.C. § 2701(a).

Consequently, the Commission should limit its use of the term "interception" to only those instances where probable cause is needed under 18 U.S.C. § 2518(3) and similar provisions, and use a more generic term such as "surveillance" when discussing the full panoply of electronic surveillance activities that carriers may receive requests for assistance by law enforcement officials.

B. Helpful Policies and Procedures

Omnipoint supports many of the Commission's tentative conclusions. Indeed, Omnipoint's existing practices and policies already reflect several Commission conclusions. For example, the Commission recommends that carriers state in their internal policies and procedures

that carrier personnel must receive a court order or, under exigent circumstances, an order from a specially designated investigative or law enforcement officer, before assisting law enforcement officials in implementing electronic surveillance. NPRM ¶ 29. Omnipoint's internal policies and procedures state that, as a general rule, all information requests by law enforcement personnel must be accompanied by a court order authorizing the requested surveillance. They then list exceptions, as appropriate for each jurisdiction, for:

- (1) subpoenas, *see, e.g.*, 18 U.S.C. § 2703;
- (2) emergency oral requests for call tracing, *see, e.g., id.* § 3125; and
- (3) written certifications, *see, e.g., id.* §§ 2511(2)(a)(ii)(B), 2518(7) (non-espionage surveillance); 50 U.S.C. §§ 1802(a)(4), 1805(e) (espionage surveillance).

As noted above, court orders and written certifications are not the only appropriate means of legal process for electronic surveillance. Consequently, Omnipoint recommends that the Commission modify its proposed requirement to reflect the other means of legal process, too.

The Commission also recommends that carriers designate specific employees, officers, or both to assist law enforcement officials in implementing lawful interceptions and that their internal policies and procedures state that, as a general rule, only designated employees may participate in lawful interception activities. NPRM ¶ 30. Omnipoint's response to law enforcement's requests for assistance are supervised by its Manager for Public Safety Affairs who is a former career law enforcement officer. Omnipoint has created policies and procedures to ensure that all aspects of lawful surveillance activities are appropriately documented and handled in a confidential manner.

The Commission also recommends that the records (not affidavits) carriers must maintain about all interceptions be compiled contemporaneously with each interception, or within 48 hours of the start of each interception, and contain certain items of information, including the name of the judge or prosecuting attorney signing the authorization. NPRM ¶ 32. Omnipoint already maintains similar records, and believes that this type of procedure is necessary to facilitate responsible carrier cooperation with law enforcement personnel.

C. Potentially Burdensome and Unnecessary Policies and Procedures

There are a number of tentative Commission conclusions that Omnipoint believes will be unduly burdensome and impractical if adopted.

First, the Commission proposes that carriers incorporate into their policies and procedures the list of exigent circumstances found at 18 U.S.C. § 2518(7). NPRM ¶ 29. This is unnecessary unless carrier personnel are expected to independently evaluate whether the requisite exigent circumstances exist before furnishing surveillance assistance to law enforcement officials who present a written certification instead of a court order. Incorporating this legal standard into carrier policies and procedures will only serve to confuse engineers and other non-lawyer carrier personnel responsible for surveillance assistance.

Current law certainly does not require such second guessing or confusion. Section 2511(2)(a)(ii)(B) of title 18, United States Code, authorizes a carrier to assist law enforcement officials to engage in electronic surveillance if such officials furnish the carrier with a certification in writing stating (a) that no warrant or court order is required by law, (b) that all statutory requirements have been met, and (c) that the specified assistance is required. There is no obligation upon the carrier to review the facts underlying the certification to determine independently that exigent circumstances justify the non-court authorized surveillance. Rather, carriers protect themselves and their employees from criminal prosecution or civil liability for alleged improper cooperation with law enforcement officials by (1) insisting upon a written demand for cooperation, (2) examining the written demand to ensure that it constitutes a facially valid certification (or, in other instances, a court order or subpoena), and (3) acting within the scope of such certification (or court order or subpoena).

Consequently, Omnipoint suggests that the Commission not require that carriers incorporate into their policies and procedures the list of exigent circumstances found at 18 U.S.C. § 2518(7).

Second, the Commission proposes that each carrier's internal policies and procedures require each employee and officer who will knowingly engage in an interception activity to sign a detailed affidavit *prior* to each instance of participation in a communications interception. NPRM ¶ 31. This requirement would unnecessarily delay the start of interceptions without significantly adding any safeguards to the proposed requirement that carriers compile records contemporaneously with each interception, or within 48 hours of the start of each interception. *Cf.* NPRM ¶ 32. Even without a notarization requirement, requiring that every carrier employee and officer responsible for the interception activity execute an affidavit before telephone company personnel respond to a request for surveillance assistance made at 2 a.m. is unnecessary and impractical.

If the Commission chooses to impose an affidavit requirement, it should limit the number and form of "affidavits" by requiring only one sworn statement (without notarization) by the employee or officer responsible for the interception activity. If the Commission chooses not to impose an affidavit requirement, then the Commission should include the suggested statement that the employee or officer will not disclose information about the interception to any person not properly authorized by statute or court order in its proposed requirement that carriers compile records contemporaneously with each interception, or within 48 hours of the start of each interception.

Third, although not a tentative conclusion, the Commission asks for comments on the nature of the information, "if any," that carriers should be required to make available to law enforcement officials upon request. NPRM ¶ 33. The NPRM identifies point of contact, list of designated employees, and social security number and other personal identifying information of each designated employee as possible illustrations of such information.

Omnipoint believes that "point of contact" is the only information that carriers should be required to provide to law enforcement officials. This information is directly related to the need to coordinate surveillance requests. Requiring carriers to provide other personal information

about their employees is far too intrusive. Moreover, it is the carriers, not law enforcement officials, that are responsible for employee compliance with surveillance laws while acting in the scope of their employment. In requiring carriers to ensure that only lawful surveillance occurs on their premises, carriers bear a responsibility to ensure that their employees comply with federal and state wiretapping and eavesdropping statutes. Permitting local, state, and federal law enforcement officials to compel intrusive information about carrier employees whenever it is demanded will not in any way ameliorate that duty.

However, carriers would like law enforcement's assistance in conducting background checks of their designated employees, especially those who consent to such checks. Consequently, federal and state law should authorize a carrier, in an effort to discharge its responsibility, to furnish personal identifying information about designated employees to law enforcement officials as part of conducting a background check. This would assist carriers in determining the criminal history background, if any, of their designated employees.

D. Other Issues

The Commission has asked for comments on the length of time that each interception record should be retained within the custody of each carrier, particularly in light of the 18 U.S.C. § 2518(8)(a) requirement that law enforcement officials maintain recordings of intercepted communications for a minimum of 10 years. NPRM ¶ 27. Carriers should maintain their interception records for as long as reasonably may be necessary to be used as evidence in a legal proceeding. Provided that no restrictions are placed on the ability of carriers to avail themselves of new information storage technologies, a requirement that each carrier retain each interception record for a minimum of ten years would be appropriate.

The Commission suggests that telecommunications carriers such as Omnipoint submit their security and recordkeeping policies to the Commission for review, NPRM ¶ 34, while some smaller carriers (whose status is determined by applying the 47 U.S.C. § 32.9000 indexed revenue threshold) need only elect between (i) filing a statement describing their security

policies, processes, and procedures, or (ii) certifying that they observe procedures consistent with the FCC's prescribed systems security rules. NPRM ¶ 35. Given that law enforcement officials consider all electronic surveillance to be important, and that all telecommunications carriers are equally responsible for cooperating with lawful requests for surveillance assistance, Omnipoint believes that the Commission should treat all carriers the same in connection with their CALEA security policies and practices obligations. Consequently, the Commission should require all carriers to submit their security and recordkeeping policies to the Commission for review, as mandated by 47 U.S.C. § 229(b)(3).

The Commission should structure its compilation of carrier security and recordkeeping policies in such a manner so as to ensure that these sensitive, confidential records are not made publicly available under the Freedom of Information Act, 5 U.S.C. § 552. For example, the Commission may wish to provide carriers the opportunity to furnish such records voluntarily so as to avail themselves of the protections afforded to business information under Critical Mass Energy Project v. NRC, 975 F.2d 871 (D.C. Cir. 1992)(en banc), *cert. denied*, 113 S.Ct. 1579 (1993).

II. Definition of Telecommunications Carrier

CALEA applies only to "telecommunications carriers." The Commission has asked for comments on the extent to which resellers should be included in CALEA's definition of "telecommunications carrier." NPRM ¶ 17.

Omnipoint believes that resellers should be included within CALEA's definition of "telecommunications carrier" to the extent that they can assist law enforcement officials conduct lawful surveillance activities. For example, resellers maintain the records that reveal dialing information and other "call-identifying information" in connection with the customers. Justice Department records reveal that the number of requests for toll records and for assistance in "call tracing" far outnumber the requests for assistance in conducting interceptions. Consequently, resellers should be included within CALEA's definition of "telecommunications carrier" to the

extent necessary to ensure effective assistance to law enforcement officials conducting lawful surveillance activities.

III. Extension of Compliance Date

Omnipoint supports the Commission's proposal to use the criteria set forth in 47 U.S.C. § 1008(b)(1) to determine whether it is reasonably achievable for a petitioner to comply with the capability requirements within the compliance time period. See NPRM ¶ 50.

Omnipoint suggests that an additional factor the FCC should consider in making this determination is whether the vendor that supplies the carrier with facilities equipment has equipment available that complies with CALEA. It can hardly be said that compliance with CALEA's assistance capability requirements is reasonably achievable within the compliance time period if the manufacturer of the carrier's equipment does not have CALEA-complaint equipment available yet.

Respectfully submitted,

OMNIPOINT COMMUNICATIONS, INC.

By:



Ronald L. Plesser
Of Counsel

Emilio W. Cividanes
Piper & Marbury, L.L.P.
1200 19th Street, N.W.
Washington, DC 20036
(202)861-3900

Its Attorneys

Date: December 12, 1997